**GIRARD SHARP LLP**
Adam E. Polk (State Bar No. 273000)
Patrick T. Johnson (State Bar No. 329580)
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: apolk@girardsharp.com
Email: pjohnson@girardsharp.com

*Counsel for Plaintiffs*

*[Additional Counsel Listed in Signature Block]*

**GIBBS LAW GROUP LLP**
David Berger (State Bar No. 277526)
Jane Farrell (State Bar No. 333779)
Sarah E. Hillier (*pro hac vice* forthcoming)
Jennifer Sun (State Bar No. 354276)
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: 510-350-9700
Email: dmb@classlawgroup.com
Email: jgf@classlawgroup.com
Email: seh@classlawgroup.com
Email: jsun@classlawgroup.com

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

CHRISTINA SPICUZZA, E.S., AND C.S., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

POWERSCHOOL HOLDINGS, INC. AND POWERSCHOOL GROUP LLC,

Defendants.

Case No:

**CLASS ACTION COMPLAINT FOR:**

1. NEGLIGENCE
2. NEGLIGENCE PER SE
3. BREACH OF IMPLIED CONTRACT
4. VIOLATION OF THE CALIFORNIA PRIVACY RIGHTS ACT, Civ. Code § 1798.100 *et seq*.
5. VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Civ. Code § 56 *et seq*.
6. VIOLATION OF THE UNFAIR COMPETITION LAW, Bus. & Prof. Code § 17200 *et seq*.

**DEMAND FOR JURY TRIAL**

Plaintiffs Christina Spicuzza, E.S., and C.S. ("Plaintiffs"), individually and on behalf of the proposed class defined below, bring this action against Defendant PowerSchool Holdings, Inc. and Defendant PowerSchool Group LLC ("PowerSchool" or "Defendants") and alleges as follows:

## I. SUMMARY OF THE ACTION

1. PowerSchool is the largest provider of cloud-based education software in the United States. It is used by more than 18,000 customers, primarily K-12 school districts and educators, to support more than 50 million students— more than 75% of K-12 students in North America. As part of its business, PowerSchool maintains in its computer systems the personally identifying information ("PII" or "Private Information") and/or protected health information ("PHI") of 60 million people, including teachers, students, and their guardians.

2. Despite holding the highly sensitive personal information of millions of people—many of whom are minors—PowerSchool left gaping cybersecurity holes. Unbeknownst to its end users PowerSchool stored PII and PHI in either unencrypted or inadequately encrypted formats on an Internet-accessible environment that did not support multi-factor authentication and allowed hackers to access and then exfiltrate vast amounts of data from that environment.

3. At some point between December 19 and December 28, 2024, hackers breached the company's vulnerable systems and exfiltrated the valuable PII and PHI stored within (the "Data Breach" or "Breach"). PowerSchool learned of the Data Breach on December 28, 2024, and began to investigate. Beginning on January 8, 2025, PowerSchool began notifying customers that their data was accessed, and that they were impacted.

4. Now, Plaintiffs and other members of the proposed class must deal with the fallout. The attack exposed over 60 million individuals' PII and PHI in total. According to public reports, the hacker claimed to have taken data on 62,488,628 students and 9,506,624 teachers in North America.[1] PowerSchool has neither confirmed nor denied the accuracy of these

[1] Lawrence Abrams, *PowerSchool hacker claims they stole data of 62 million students*, BleepingComputer, January 22, 2025, https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/.

numbers, nor has it identified the precise number of these victims that reside in the United States.

5. The Private Information stolen in the Data Breach includes dates of birth, addresses, phone numbers, emails, photo identification, and tax information numbers. The hackers obtained Social Security numbers for roughly 25% of the class, putting them at risk for a vast array of identity theft and fraud for years to come. The hackers obtained an unknown number of victims' health histories and other medical information. Plaintiffs' information continues to reside on or remain accessible through PowerSchool's systems.

6. Plaintiffs by this action seek compensatory and statutory damages as well as injunctive relief to remediate PowerSchool's deficient cybersecurity and provide credit monitoring, identity theft insurance, and credit repair services (or the money needed to secure those services) to protect them and the other breach victims from identity theft and fraud.

## II. PARTIES

7. Plaintiff C.S. is a minor under the age of 18. At all relevant times, C.S. has been domiciled in the state of California. Plaintiff C.S. attends school in the Cambrian School District.

8. Plaintiff E.S. is a minor under the age of 18. At all relevant times, E.S. has been domiciled in the state of California. Plaintiff E.S. attends school in the Cambrian School District

9. Plaintiff Christina Spicuzza is the mother and legal guardian of Plaintiffs C.S. and E.S. At all relevant times, she has been domiciled in the state of California.

10. Defendant PowerSchool Holdings, Inc., is a Delaware corporation with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

11. Defendant PowerSchool Group LLC is a Delaware Limited Liability Company with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

12. Defendant PowerSchool Holdings, Inc. and PowerSchool Group LLC are collectively referred to as PowerSchool or Defendants.

13. At all relevant times, each Defendant was a principal, agent, alter ego, joint venturer, partner, or affiliate of each other, and in doing the acts alleged herein, was acting within the course and scope of that principal, agent, alter ego, joint venture, partnership, or

affiliate relationship. Each Defendant had actual knowledge of the wrongful acts of each other; ratified, approved, joined in, acquiesced, or authorized the wrongful acts of each other; and retained the benefits of those wrongful acts.

## III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' states of citizenship.

15. This Court has personal jurisdiction over Defendants because they conduct substantial business and have minimum contacts with the State of California.

16. Venue is proper in this District under 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

## IV. FACTUAL BACKGROUND

### A. Background on PowerSchool

17. PowerSchool holds itself out "[a]s a leading provider of cloud-based software in North America." Its product supports vast numbers of teachers, students, and their parents. Seventy-five percent of American school children, over 35 million, use PowerSchool. Over 16,000 customers rely on PowerSchool, including 90 of the largest 100 districts by student enrollment.

18. PowerSchool built itself into a market leader in "secure" education technology. It was so successful that in 2024, Bain Capital acquired PowerSchool for $5.6 billion.

19. The data PowerSchool collects far exceeds traditional education records of school-age children, including thousands of person-specific data fields.

20. PowerSchool does not fully disclose what data it collects from school-age children or their parents.

21. PowerSchool refuses to provide children and parents access to their data or the information it generates using that data.

22. PowerSchool collects and maintains the PHI and PII of customers, including but not limited to:

a. name, residential address, phone number, and email address
b. date of birth
c. demographic information
d. Social Security number
e. tax identification number
f. financial information
g. medication information
h. disability information
i. health insurance information
j. photo identification
k. employment information

23. Indeed, the stolen data even included personal information regarding parental access rights to children, parental restraining orders, and instructions about when certain students need to take medication.[2]

**B. The *Data Breach***

24. As of this writing, PowerSchool has provided scant information about what happened in the data breach – but the available information shows serious gaps in PowerSchool's information security controls.

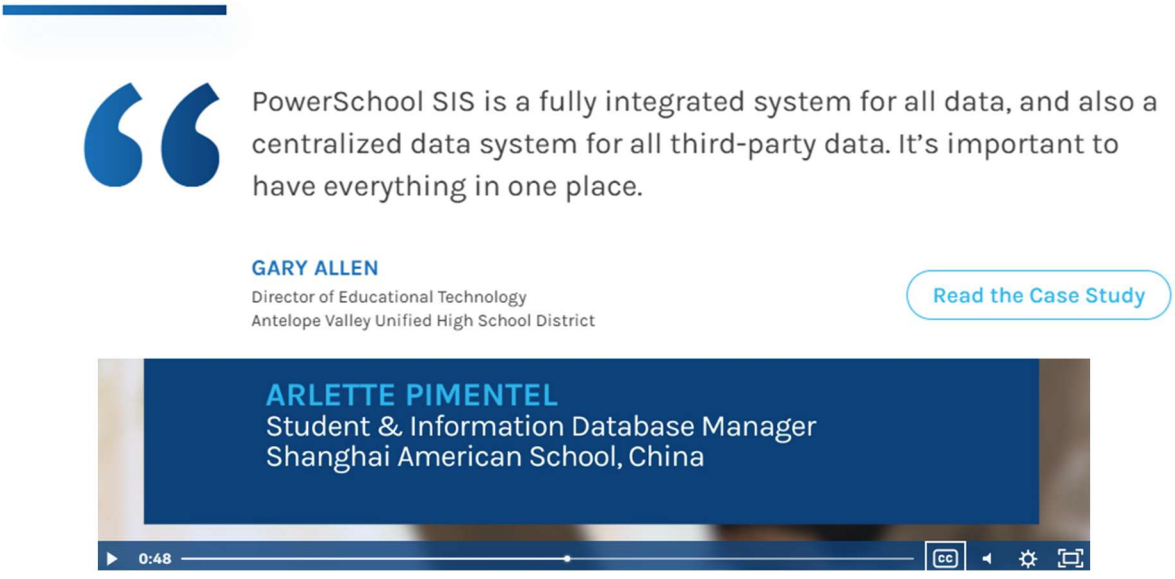
25. On December 19, 2024, financially motivated hackers used compromised credentials to access PowerSource, a "community-focused customer portal." When used appropriately, PowerSource "is available to all district and school staff, including teachers, administrators and IT staff." PowerSchool has admitted that at the time of the data breach,

[2] Carly Page, What PowerSchool isn't saying about its 'massive' student data breach, TechCrunch, Jan. 22, 2025, https://techcrunch.com/2025/01/22/what-powerschool-isnt-saying-about-its-massive-student-data-breach/.

PowerSource did not support (let alone require) multi-factor authentication, a standard information security control that on its own would have prevented this Data Breach.

26. The hackers then spent the next couple of weeks conducting reconnaissance in the PowerSchool environment. Failing to notice active hacking over weeks indicates that PowerSchool either lacked standard intrusion detection systems adequate to notice this suspicious activity or that PowerSchool personnel failed to heed the warning of their systems. If PowerSchool had properly implemented and configured these standard information security controls, this Data Breach would not have happened or would have been halted before the data was exfiltrated.

27. Moreover, PowerSource was configured to allow users to access the vast array of data that PowerSchool stored in its PowerSchool SIS system. PowerSchool's marketing emphasizes that their Student Information System ("SIS") operates as, essentially, a one-stop shop for all student data. The marketing materials for PowerSchool SIS describe it as "one secure customizable platform providing the interoperability needed to power your school and district operations with accurate student data."



28. PowerSchool SIS gathers data on students and families directly from students and their families as it provides the platform families use for online enrollment in its customers' schools and districts.

29. PowerSchool SIS also gathers data on students and families from its customers and their employees, including data on "attendance, behavior, health, graduation tracking, asset tracking, and student demographics."

30. From a cybersecurity perspective, it is inexcusable that a company would allow access to such sensitive information through an internet-facing portal that is not protected by multi-factor authentication. But PowerSchool's security failings are far worse than just this.

31. Typically, when hackers are able to use stolen credentials, they are able to get access to whatever data the rightful owner of those credentials would be permitted to see. Here, however, the hackers were able to access the collective data of thousands of different users. This indicates either that PowerSchool's systems were internally misconfigured to permit dangerously broad access or that PowerSchool failed to prevent the theft of high-level administrative credentials, which should have required multiple security controls to use.

32. On December 22, the hackers used a data export tool normally used for remote support to create and export two massive data files: students_export.csv and teachers_export.csv. Once again, standard information security controls should have prevented this activity. For example, PowerSchool should have implemented Data Loss Prevention (DLP) technology that would have noticed this data aggregation, particularly from so many different customers, and halted the action. A DLP solution also would have integrated with PowerSource's intrusion detection systems to immediately alert information security personnel to the hackers' presence. Again, these are standard information security controls that any entity hosting massive quantities of Private Information should have implemented.

33. In fact, PowerSchool's security was so poor that it allowed the hackers to obtain data from PowerSchool customers that hosted their own data on their own servers around the country. As long as they were using PowerSchool SIS, they were vulnerable.

34. Once the hackers had aggregated millions of records into these two files, they exfiltrated the data without PowerSchool ever noticing such massive data transfers. Properly implemented intrusion detection and DLP tools would have stopped the hackers from obtaining the data files. But PowerSchool's information security controls again failed.

35. PowerSchool never even learned of the Data Breach until December 28, 2024, when the hackers contacted PowerSchool to seek a ransom in exchange for purportedly deleting the data.

36. PowerSchool investigated the Data Breach and identified the compromised products and customers. It confirmed that the breach affected "families and educators" and various types of sensitive Private Information, including "the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information."

37. On January 8, 2025, PowerSchool publicly announced the Data Breach and began notifying customers.

**C. PowerSchool's Data Security Representations**

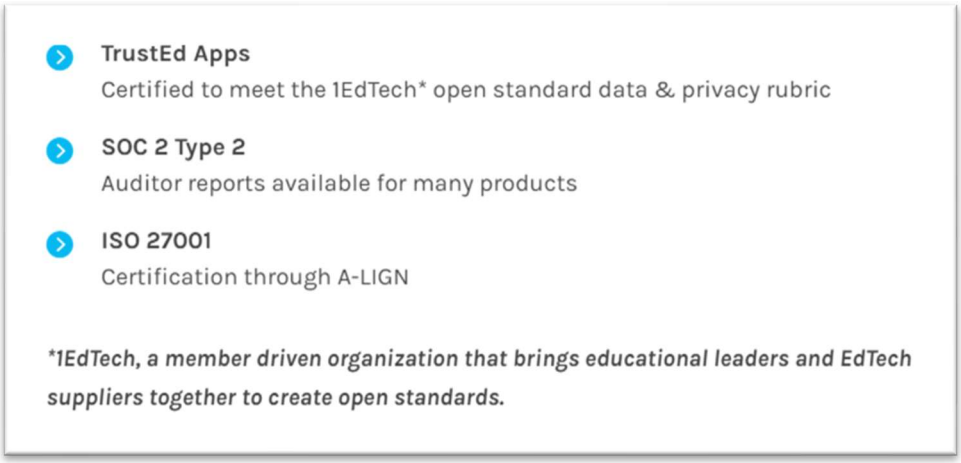
38. PowerSchool knew its obligations in ensuring data security and understood the importance of "safe collection and management of student data."[3]

[3] PowerSchool, *Top 6 Best Practices for Improving Student Information System (SIS) Cybersecurity*, Sept. 10, 2024, https://www.powerschool.com/blog/best-practices-improving-sis-cybersecurity/.


39. For example, the marketing video with which PowerSchool advertises PowerSchool SIS includes an emphasis on the security of PowerSchool SIS[4]:


[4] "PowerSchool SIS at-a-glance," video found at https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited January 21, 2025).

40. PowerSchool has multiple webpages dedicated to its privacy and security capabilities. It represents that it uses "industry standards" to "improve data integrity and security."[5] It claims that all products are "[c]ertified to meet the 1EdTech open standard data & privacy rubric," and have received "ISO 27001" certification through "A-LIGN."




41. The top line of its "Cybersecurity, Data Privacy, and Infrastructure" webpages state that "PowerSchool is committed to being a good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[6]

42. In its privacy policy, PowerSchool boasts that it "places great importance and value on the proper handling of personal data that flows within our product as we provide services to our customers."[7] To this end, PowerSchool claims that it has the "relevant security and privacy policies to drive expectations from the workforce":

> We seek to protect our customers' personal data from unauthorized access, use, modification, disclosure, loss, or theft by leveraging various reasonable security measures and methods to secure our customers' personal data throughout its processing lifecycle with PowerSchool applications. Our overall aim is to ensure the confidentiality, integrity, and availability of our customers' personal data by leveraging technical,

[5] https://www.powerschool.com/interoperability-overview/ (last visited February 7, 2025).
[6] "PowerSchool's Privacy Principles," PowerSchool, https://www.powerschool.com/privacy/ (last visited January 21, 2025).
[7] https://www.powerschool.com/privacy/ (last visited February 7, 2025).

> organizational, and where appropriate, physical security methods. Security protection at PowerSchool is a cross-functional activity that intersects our workforce duties, and we have relevant security and privacy policies to drive expectations from the workforce.[8]

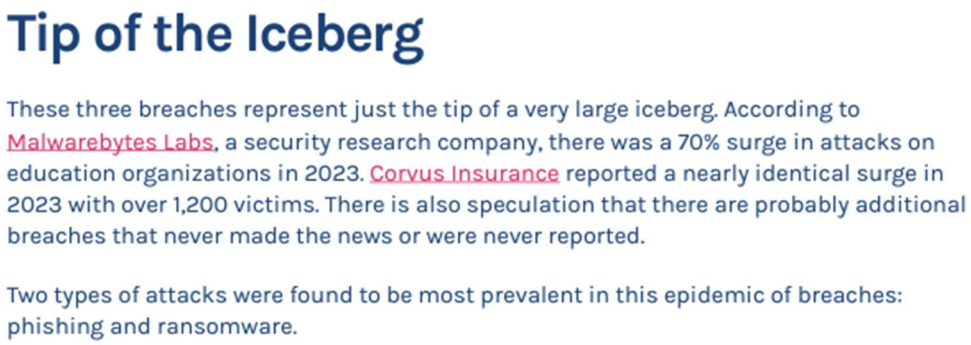
43. Under the "Frequently Asked Questions," PowerSchool represents that it protects data by using "state-of-the-art, and appropriate physical, technical, and administrative security measures to protect the personal data that we process."[9]

44. PowerSchool's Global Privacy Statement, last updated October 1, 2024, makes the following representations about PowerSchool's data security measures:

> Whether PowerSchool is a collector or processor or your data, PowerSchool is committed to protecting your personal information. PowerSchool uses commercially reasonable physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and availability of your personal information. Our systems are regularly certified by third parties against industry security standards from AIPCA and ISO. As customers provide PowerSchool with Customer Data to process, PowerSchool makes commercially reasonable efforts to ensure the security of our systems. Please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, administrative, and technical safeguards.
> …
> PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. We strive to continuously maintain reasonable physical, administrative, and technical security measures. Our security measures consider the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data. PowerSchool independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications. PowerSchool also endeavors to align its privacy and security operations to best practices and relevant international regulations.[10]

[8] *Id.*
[9] *Id.*
[10] *Id.*

45. In "PowerSchool: A Leader in Responsible AI for Education," a PDF linked on its website, PowerSchool states: "As the education sector has become more reliant on digital technologies, we face increasing cybersecurity threats from hackers who seek to exploit vulnerabilities, steal data, or disrupt operations." PowerSchool mentions three school cybersecurity attacks that occurred in 2023 and notes that these are "just the tip of a very large iceberg."[11]



## Tip of the Iceberg

These three breaches represent just the tip of a very large iceberg. According to Malwarebytes Labs, a security research company, there was a 70% surge in attacks on education organizations in 2023. Corvus Insurance reported a nearly identical surge in 2023 with over 1,200 victims. There is also speculation that there are probably additional breaches that never made the news or were never reported.

Two types of attacks were found to be most prevalent in this epidemic of breaches: phishing and ransomware.

46. In a section of the PDF discussing ransomware threats, PowerSchool specifically advises readers to not pay a ransom or negotiate with hackers because "[p]aying the ransom does not guarantee that you will get your data back, or that it will not be leaked or sold. It also … makes you a more attractive target for future attacks."[12]

**D. PII and PHI have concrete financial value**

47. PHI and PII are inherently valuable, and they are becoming increasingly frequent targets of hackers. The PII and PHI taken from PowerSchool's systems are particularly sensitive.

48. Medical records and personally identifiable information are valuable to cybercriminals and routinely are sold and traded on the dark web. There is a robust black market in which criminals openly post stolen PHI and PII on multiple underground internet websites, commonly referred to as the dark web.

---

[11] "PowerSchool: A Leader in Responsible AI for Education," June 10, 2024, https://go.powerschool.com/rs/861-RMI-846/images/Responsible_AI_Cybersecurity_Report.pdf?version=0 (last visited January 22, 2025).

[12] *Id.*

49. Identity theft results in a significant, negative financial impact on victims as well as severe distress.

50. PHI and PII are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes, including identity theft and medical and financial fraud. There is accordingly a market for Plaintiffs' and Class members' PHI and PII.

51. PHI is particularly sensitive. Healthcare data can sell for as much as $363 per record, according to the Infosec Institute.[13] PHI is especially valuable because criminals can use it to target victims with fraud and scams that take advantage of the victim's medical conditions or settlements. PHI can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or to gain access to prescriptions for illegal use or resale.

52. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, misdiagnosis or mistreatment can ensue. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," said Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[14]

53. Similarly, Social Security numbers are valuable to criminals. This information can be, and has been, sold and traded on the dark web. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

54. The detrimental consequences of PowerSchool's failure to keep its customers', students', families', and educators' PHI and PII secure are long lasting and severe. Once PHI and

[13] https://resources.infosecinstitute.com/topics/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/ (last accessed February 7, 2025).

[14] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last accessed February 7, 2025).

PII are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or years.

55. Children are particularly vulnerable targets in a data breach. Identity theft can result in malicious actors running up debts before the child even turns 18. The child might be unaware of these debts until years later when they enter into the credit market to apply for loans or financial aid.

56. Criminals often trade stolen PHI and PII on the dark web for years following a breach. Cybercriminals also can post stolen PHI and PII on the internet, thereby making the information publicly available without the knowledge or consent of the victim.

57. PowerSchool knew the importance of safeguarding the PHI and PII entrusted to it and the foreseeable adverse effects if its data security systems were breached. Those effects include the significant costs that would be imposed on affected students, their parents, and educators as a result of a breach. PowerSchool failed to implement reasonable and adequate cybersecurity measures, leading to the Data Breach.

**E. PowerSchool Owed Duties to Safeguard Individuals' PII and PHI**

58. Beyond the obligations arising from PowerSchool's own representations keeping Plaintiffs' and Class Members' data secure, Defendants owed Plaintiffs and Class members a duty to safeguard their PII and PHI.

59. As described further below, Defendants owed a duty to safeguard PII and PHI under several statutes, including the Federal Trade Commission Act ("FTC Act") and the Children's Online Privacy Protection Act ("COPPA"), to ensure that all information they maintained was secure. These statutes were enacted to protect Plaintiffs and the Class members from the type of conduct in which Defendants engaged.

60. Defendants owed a duty to safeguard PII and PHI because they were on notice that they were handling highly valuable data and knew there was a risk it would be targeted by cybercriminals. Moreover, Defendants knew of the extensive, foreseeable harm that would ensue for the victims of a data breach and therefore owed a duty to safeguard that information.

61. Given the sensitive nature of the PII and PHI routinely contained in Defendants' systems, Defendants knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially engineered attacks, healthcare fraud, and other identity-related fraud upon exfiltrating that data from Defendants' system. Defendants also knew that individuals whose PII and PHI were maintained Defendants' system would reasonably spend time and effort to mitigate their damages and prevent identity theft and fraud, if that PII and PHI were taken.

62. Defendants also owed a duty to safeguard Plaintiffs' and Class members' data based upon the promises that they made to their clients and customers to securely store data. Defendants voluntarily undertook efforts to keep that data secure in their business operations and thus owe a continuing obligation to Plaintiffs and Class members to keep their PII and PHI secure.

63. The duty to protect Plaintiffs' PII and PHI is non-delegable. PowerSchool's business model is premised upon voluntarily assuming this duty, by soliciting customers to rely on its professed ability to store sensitive data securely. PowerSchool's duty is for the benefit of the individuals whose PII and PHI its products store and manage.

64. Defendants also owed a duty to comply with industry standards in safeguarding PII and PHI, which they did not do.

65. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining, or securing PII and PHI such as Defendants, have been identified as being particularly vulnerable to cyberattacks. Cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

66. Federal and state government bodies have likewise established security standards and issued recommendations to reduce the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for businesses highlighting the importance of robust and effective data and cyber security practices. According to the FTC, the imperative of data and cyber security should be factored into all business decision-making.

67. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data and cyber security principles and practices for business. The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines further recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

68. The FTC also recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ appropriate measures to protect against unauthorized access to confidential consumer data as an unfair practice that violates Section 5 of the FTC Act, 15 U.S.C. § 45. Orders in these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

70. Further, under COPPA, 15 U.S.C. § 312.10, Defendants had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to

fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

**F. Plaintiffs' PHI and PII were Compromised in the Data Breach**

71. Plaintiff Christina Spicuzza is C.S. and E.S.'s parent and legal guardian. All Plaintiffs are citizens and residents of San Jose, California. C.S. and E.S. attend school in the Cambrian School District.

72. As part of C.S. and E.S.'s schooling, Plaintiff Spicuzza provided PowerSchool her children's sensitive PII and PHI and provided sensitive PII of herself.

73. On January 10, 2025, and January 14, 2025, Plaintiffs received an email from the Cambrian School District stating that PowerSchool had informed them that the school district had been affected by the Data Breach. The district's notice conveyed PowerSchool's representations that it had "contained" the incident.

74. Plaintiffs greatly value their privacy, and Plaintiff Spicuzza values the privacy of her minor children. Because of PowerSchool's failure to protect the sensitive information entrusted to it, Plaintiffs are less safe now than they were before the breach.

75. Plaintiff Spicuzza has suffered actual injury in the form of damages to, and diminution in, the value of her PII and the PII of her children — a form of intangible property that she entrusted to PowerSchool in exchange for education support and administration services.

76. The exposure of Plaintiffs' private and confidential information, including health information, in the Data Breach has caused Plaintiffs to suffer stress and anxiety related to her family's personal information being compromised.

77. Plaintiffs have suffered imminent and impending injuries arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and PHI especially with her children's Social Security number indefinitely in the hands of criminals.

78. Because of the Data Breach, Plaintiffs are at a substantial present risk both with respect to their personal safety and increased risk of identity theft and fraud and will continue to face an increased risk for years to come.

79. Plaintiffs and Class members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

80. Plaintiffs have a continuing interest in ensuring that their PII and PHI, which remain in PowerSchool's possession, are protected and safeguarded from future breaches.

## V. CLASS ACTION ALLEGATIONS

81. Plaintiffs bring this class action on behalf of themselves and all others similarly situated pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and where applicable, 23(c)(4), on behalf of the following Nationwide Class and California subclass (collectively, the "Class"):

> **Nationwide Class:** All natural persons in the United States whose PII and/or PHI was compromised as a result of the Data Breach.
>
> **California Class:** All persons residing in California whose PII and/or PHI was compromised as a result of the Data Breach.

82. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

83. Plaintiffs reserve the right to modify the Class definition, including based on discovery and further investigation.

84. Numerosity. The Class is so large as to make joinder impracticable. There are millions of Class members. Disposition of their claims in a single action will provide substantial

benefits to all parties and to the Court. Class members are readily ascertainable from information and records in the possession, custody, or control of Defendants or its customers.

85. Typicality. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class members, was compromised and stolen in the Data Breach.

86. Adequacy of Representation. Plaintiffs are members of the Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in prosecuting class actions, including relating to data breaches. Plaintiffs have no interest contrary to or in conflict with the interests of Class members.

87. Predominant Common Issues of Law and Fact. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

- Whether Defendants engaged in the conduct alleged;
- Whether Defendants had a duty to implement reasonable cyber security measures to protect Plaintiffs' and Class members' sensitive, personal information;
- Whether Defendants breached their duty by failing to take reasonable precautions to protect Plaintiffs' and Class members' sensitive, personal information;
- Whether Defendants acted unfairly or otherwise wrongfully in violation of state statutory law;
- Whether Plaintiffs and Class members are entitled to recover damages; and
- Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, and/or disgorgement.

88. Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Given the relatively small size of the individual Class members' claims, few, if any, Class members would seek redress for Defendants' violations individually. Class treatment will conserve the resources of the courts and promote consistency and efficiency of adjudication.

Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendants.
- The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests.
- Defendants have acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declarative relief appropriate with respect to the Class as a whole; and
- The claims of Class members are comprised of common issues whose resolution in a class trial would materially advance this litigation.

## FIRST CAUSE OF ACTION
### Negligence
### On Behalf of Plaintiffs and the Nationwide Class

89. Plaintiffs incorporate and reallege the foregoing allegations of fact.

90. Defendants collected and stored Plaintiffs' and Class members' personal information, including addresses, Social Security numbers, dates of birth, health insurance information, and personal health information including disabilities, immunization records, and medications.

91. Defendants owed Plaintiffs and Class members a duty of reasonable care to preserve and protect the confidentiality of their personal information that it collected. This duty included, among other obligations, maintaining and testing its security systems and networks, and the systems and networks of its vendors, as well as taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiffs and the Class from unauthorized access and use.

92. Defendants' duties also arise by operation of statute. Pursuant to the FTC Act, 15 U.S.C. § 45, PowerSchool had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PHI and PII.

93. Plaintiffs and Class members were the foreseeable victims of Defendants' inadequate and ineffectual cybersecurity systems and protocols. The natural and probable consequence of Defendants' failing to adequately secure its information networks was Plaintiffs' and Class members' personal information being hacked.

94. Defendants knew or should have known that Plaintiffs' and Class members' personal information was an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States. Moreover, the harm to Plaintiffs and Class members from exposure of their highly confidential personal information was reasonably foreseeable to Defendants.

95. Defendants had the ability to sufficiently guard against data breaches by monitoring and testing their systems and implementing adequate measures to protect their systems, such as using attack surface software.

96. Defendants breached their duty to exercise reasonable care in protecting Plaintiffs' and Class members' personal information by failing to implement and maintain adequate security measures to safeguard Plaintiffs' and Class members' personal information, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of, Plaintiffs' and Class members' confidential personal information.

97. There is a close connection between Defendants' failure to employ reasonable security protections for its members and beneficiaries' personal information and the injuries suffered by Plaintiffs and Class members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and may need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for

unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

98. Defendants were in a special relationship with Plaintiffs and Class members with respect to the hacked information because the end and aim of Defendants' data security measures was to benefit Plaintiffs and Class members by ensuring that their personal information would remain protected and secure. Only Defendants could ensure that its systems were sufficiently secure to protect Plaintiffs' and Class members' personal and medical information. The harm to Plaintiffs and Class members from their exposure was foreseeable to Defendants.

99. The policy of preventing future harm disfavors the application of the economic loss rule, particularly given the sensitivity of the private information entrusted to Defendants. A high degree of opprobrium attaches to Defendants' failure to secure Plaintiffs' and Class members' personal and extremely confidential facts. Defendants had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiffs and Class members.

100. As a result of Defendants' negligence, Plaintiffs and Class members have suffered actual and/or nominal damages that have included or may, in the future, include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2) diminution in the value and use of their personal information entrusted to Defendants with the understanding that Defendants would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (6) unauthorized use of compromised personal information to open new financial and other accounts; (7) continued risk to their

personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (8) future costs in the form of time, effort, and money Plaintiffs and Class members will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

**SECOND CAUSE OF ACTION**
**Negligence *per se***
**On Behalf of Plaintiffs and the Nationwide Class**

101. Plaintiffs incorporate and reallege the foregoing allegations of fact.

102. Under Section 5 of the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

103. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not comply with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII of their consumers.

104. Plaintiffs and Class members are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

105. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

106. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act was intended to guard against.

107. Further, under COPPA, 15 U.S.C. § 312.10, Defendants had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

108. Defendants violated COPPA § 312.10 by failing to use reasonable measures to protect PII and PHI and not complying with industry standards.

109. Plaintiffs and Class members are consumers within the Class of persons COPPA was intended to protect.

110. Defendants' violation of COPPA constitutes negligence *per se*.

111. The harm that has occurred as a result of Defendants' conduct is the type of harm that COPPA was intended to guard against.

112. As a direct and proximate result of Defendants' negligence, Plaintiffs have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

## THIRD CAUSE OF ACTION
**Breach of Implied Contract**
**On Behalf of Plaintiffs and the Nationwide Class**

113. Plaintiffs incorporate and reallege the foregoing allegations of fact.

114. Defendants contracted with Plaintiffs' and the Class members' schools and/or school districts for the provision of education software. These contracts include, without limitation, Defendants' privacy notices in which they promised to protect nonpublic personal information given to Defendants, or which Defendants gathered on their own, from disclosure. These privacy notices include Defendants' Global Privacy Statement.

115. Plaintiffs and Class members are the intended beneficiaries of those contracts, including the provisions incorporating Defendants' privacy policies and otherwise pertaining to the confidentiality of personal information maintained by Defendants.

116. Plaintiffs and Class members performed substantially all that was required of them under their contracts with Defendants, or they were excused from doing so.

117. Defendants explicitly acknowledged their obligation to protect Plaintiffs' and Class members' confidential information in these contracts. In their Global Privacy Statement, Defendants state that PowerSchool "uses commercially reasonable physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and availability of your personal information."

118. A meeting of the minds occurred, as Plaintiffs and other Class members agreed, among other things, to provide their PII and PHI to Defendants for which Defendants derived a monetary benefit, in exchange for Defendants' agreement to protect the confidentiality of that information.

119. No Plaintiff would have entered into these contracts with Defendants without understanding that Plaintiffs' and other Class members' PII and PHI would be safeguarded and protected. In short, data security was a material term of the parties' contracts.

120. Defendants breached these promises by failing to comply with reasonable industry practices, and by allowing unauthorized users to gain access to Plaintiffs' and Class members' PII and PHI through the Data Breach.

121. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received education services that were less valuable than promised in their contracts. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

122. As a result of Defendants' breach of contract, Plaintiffs and Class members have suffered actual damages resulting from the exposure of their personal information, remain imminent risk of suffering additional damages in the future, and/or are otherwise entitled to nominal damages.

123. Plaintiffs and Class members have consequently been injured by Defendants' breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial. Plaintiffs seek nominal damages in the alternative.

## FOURTH CAUSE OF ACTION
**Violation of the California Privacy Rights Act**
**Civ. Code § 1798.100 *et seq.* ("CPRA")**
**On Behalf of Plaintiffs and the California Class**

124. Plaintiffs incorporate and reallege the foregoing allegations of fact.

125. Section 1798.150(a)(1) provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

126. Plaintiffs are consumers and California residents as defined by Civil Code section 1798.140(i).

127. PowerSchool is a "business" as defined by Civil Code section 1798.140(d)(2) because it shares common branding and controls entities that are "organized or operated for the profit or financial benefit of its shareholders or other owners, that collect[] consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determine[] the purposes and means of the processing of consumers' personal information, that do[] business in the state of California."

128. Plaintiffs' and Class members' personal information, as defined by Civil Code section 1798.140(v)(1), was subject to unauthorized access and exfiltration, theft, or disclosure. The Data Breach described herein exposed, without limitation, Social Security numbers, dates of birth, addresses, phone numbers, emails, photo identification, tax information numbers, health histories, and other medical information.

129. PowerSchool maintained Plaintiffs' and Class members' PII in a form that allowed criminals to access it.

130. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Defendants failed to monitor its systems to identify suspicious activity and allowed unauthorized access to Plaintiffs' and Class members' PII.

131. Consistent with Civil Code Section 1798.150(b), Plaintiffs provided written notice to Defendants identifying the provisions that Defendants violated, and that Defendants have 30

days to cure those violations. Plaintiffs provided written notice to PowerSchool of specific violations of § 1798.150(a) by certified mail dated February 5, 2025.[15] If Defendant is unable to cure or does not cure its violations within the 30-day period required by the notice, Plaintiffs will amend this complaint to pursue actual or statutory damages, as permitted by Civil Code section 1798.150(b).

132. At this time, Plaintiffs seek actual damages, as permitted by Civil Code section 1798.150(b), injunctive and declaratory relief, and any other relief as deemed appropriate by the Court for Defendants' violations. Plaintiffs do not currently seek statutory damages for Defendants' CPRA violations but reserve the right to seek statutory damages in the future.

**FIFTH CAUSE OF ACTION**
**Violation of the California Confidentiality of Medical Information Act**
**Civ. Code § 56 *et seq*. ("CMIA")**
**On Behalf of Plaintiffs and the California Class**

133. Plaintiffs incorporate the above allegations as if fully set forth herein.

134. Under Section 56.10(a) of the Civil Code, "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining authorization[.]"

135. Defendants are a business deemed to be a "provider of health care" as defined in Civil Code section 56.06(b). Defendants are a business that offers software to consumers that is designed to maintain medical information in order to make the information available to an individual or a provider of health care for the purposes of allowing the individual to manage the individual's information, or for the treatment, or management of a medical condition of the individual. PowerSchool is a cloud-based education software used by more than 18,000 customers, primarily K-12 educators, to support more than 50 million students, including those with medical conditions and disabilities.

[15] Ex 1. (Plaintiffs Notice Letter)

136. Plaintiffs and Class members are "patients" within the meaning of Civil Code section 50.05(m) and are "enrollee[s]" within the meaning of Civil Code section 56.05(e).

137. Plaintiffs and Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code section 56.05(j), created, maintained, preserved, stored, abandoned, destroyed or disposed of on or through Defendants' software at the time of the Data Breach.

138. Defendants violated Civil Code section 56.101 by failing to maintain and preserve the confidentiality of Plaintiffs' and Class members' medical information.

139. In violation of Civil Code section 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and Class members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality. As a result, Plaintiffs' and Class members' confidential information and records were negligently released to hackers in the Data Breach.

140. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by Civil Code section 56.101(c).

141. That the information taken in the breach was viewed by unauthorized individuals is evidenced by the fact that the hackers successfully breached PowerSchool's computer systems, exfiltrated customer PII and PHI, and demanded a ransom based on viewing the stolen data to ascertain its value.

142. In violation of Civil Code section 56.101(b)(1)(A), Defendants' electronic health record systems or electronic medical record systems failed to protect and preserve the integrity of electronic medical information.

143. Defendants also violated Civil Code section 56.36(b) by negligently releasing Plaintiffs' and Class members' confidential information in the Data Breach.

144. Defendants' wrongful conduct, actions, inaction, omissions, and want of ordinary care violate the CMIA and directly and proximately caused the Data Breach. Plaintiffs and Class members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their

medical information; (2) loss of the opportunity to control how their medical information is used; (3) diminution in the value and use of their medical information entrusted to Defendants with the understanding that Defendants would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identify theft and misused of their medical information; (5) continued undue risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their medical information being stolen in the Data Breach.

145. Plaintiffs and Class members were injured and have suffered damages, as described above, from Defendants' negligent release of their medical information in violation of Civil Code sections 56.36 and 56.101 and accordingly are entitled to relief under Civil Code 56.36, including actual damages, nominal statutory damages of $1,000, injunctive relief, and attorney fees, expenses, and costs.

**SIXTH CAUSE OF ACTION**
**Violation of the Unfair Competition Law**
**Bus. & Prof. Code § 17200 *et seq*. ("UCL")**
**On Behalf of Plaintiffs and the California Class**

146. Plaintiffs incorporate the above allegations as if fully set forth herein.

147. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

148. Defendants' conduct is unlawful, in violation of the UCL, because it violates the CPRA and CMIA.

149. Defendants' conduct also is unfair and deceptive in violation of the UCL. Defendants' unfair and fraudulent business acts and practices include:

a. Failing to adequately secure the personal information of Plaintiffs and Class members from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts about Plaintiffs and Class members in a manner highly offensive to a reasonable person;

c. Enabling the disclosure of personal and sensitive facts about Plaintiffs and Class members without their informed, voluntary, affirmative, and clear consent;

d. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiffs' and Class members' personal information.

150. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of Plaintiffs' and Class members' personal information.

151. The gravity of harm resulting from Defendants' unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

152. The harm from Defendants' conduct was not reasonably avoidable by Plaintiffs and Class members. The persons affected by the Data Breach—teachers, students, and their parents—were required to provide their PII to support the information system that schools use to manage student records, grades, attendance, and enrollment. Plaintiffs and Class members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through in adequate data security measures.

153. There were reasonably available alternatives that would have furthered Defendants' business interests of electronically transferring their customers' information while protecting PII.

154. A reasonable person would regard Defendants' derelict data security and the Data Breach as important, material facts that could and should have been disclosed.

155. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs lost money or property because their sensitive personal information experienced a diminution of value and because they devoted additional time to monitoring their financial accounts for fraudulent activity.

156. Plaintiffs and Class members therefore seek all monetary and non-monetary relief permitted by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs under Code of Civil Procedure section 1021.5.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs pray for an order:

A. Certifying this case as a class action, appointing Plaintiffs as a Class representative, and appointing Plaintiffs' counsel to represent the Class;

B. Entering judgment for Plaintiffs and the Class;

C. Awarding Plaintiffs and Class members monetary relief, including nominal and statutory damages;

D. Ordering appropriate injunctive or other equitable relief;

E. Awarding pre- and post-judgment interest as prescribed by law;

F. Awarding reasonable attorneys' fees and costs as permitted by law; and

G. Granting such further and other relief as may be just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: February 7, 2025

Respectfully submitted,

By: /s/ *Patrick T. Johnson*

Adam E. Polk (State Bar No. 273000)
Patrick T. Johnson (State Bar No. 329580)
**GIRARD SHARP LLP**
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: apolk@girardsharp.com
Email: pjohnson@girardsharp.com

David Berger (State Bar No. 277526)
Jane Farrell (State Bar No. 333779)
Sarah E. Hillier (pro hac vice forthcoming)
Jennifer Sun (State Bar No. 354276)

**GIBBS LAW GROUP LLP**
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: 510-350-9700
Email: dmb@classlawgroup.com
Email: mht@classlawgroup.com
Email: jgf@classlawgroup.com
Email: seh@classlawgroup.com
Email: jsun@classlawgroup.com

Mark H. Troutman (*pro hac vice* forthcoming)
**GIBBS LAW GROUP LLP**
1554 Polaris Parkway, Suite 325
Columbus, Ohio 43240
Telephone: (510) 350-9700
Fax: (510) 350-9701
Email: mht@classlawgroup.com

M. Anderson Berry (State Bar No. 262879)
**CLAYEO C. ARNOLD A PROFESSIONAL CORPORATION**
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 239-4778
Email: aberry@justice4you.com

*Counsel for Plaintiffs*

# EXHIBIT 1

GIRARD SHARP

February 5, 2025

**VIA FIRST CLASS MAIL**

PowerSchool
Hardeep Gulati, CEO
150 Parkshore Drive,
Folsom, CA 95630

Re: Christina Spicuzza CCPA Demand Letter

To Whom It May Concern:

We represent Christina Spicuzza and her children E.S., and C.S. ("Plaintiffs"), along with a proposed class of similarly situated consumers in connection with the breach of PowerSchool on or about December 19 and December 28, 2024. PowerSchool provides cloud-based education software. To perform these functions, PowerSchool maintains in its computer systems the personally identifying information ("PII") and/or protected health information ("PHI"). PowerSchool learned of the breaches to its electronic information systems that compromised millions of people's most sensitive information (the "Data Breach").

Our clients, Christina Spicuzzi, E.S., and C.S., are residents of San Jose, California. Plaintiff Christina Spicuzza is the mother and legal guardian of Plaintiffs C.S. and E.S. Plaintiffs received notice from their school district on January 10, 2025 stating that PowerSchool had informed them that the school district had been affected by the Data Breach.

PowerSchool's conduct constitutes violations of California Civil Code sections 1798.81.5(b) and 1798.150(a)(1). In accordance with California Civil Code section 1798.150(b), in the event that a cure is possible, Plaintiff provides PowerSchool the opportunity to cure the noticed violations and provide an express written statement that the violations have been cured and that no further

violations will occur. A cure, if possible, would require PowerSchool to recover all stolen PII and PHI and eliminate any future risk that Plaintiffs' and Class members' stolen PII or PHI is misused.

Very truly yours,

**GIRARD SHARP LLP**

Adam E. Polk